(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 459 046 A1**

(12) **EUROPEAN PATENT APPLICATION**

(21) Application number: **90305964.0**

(51) Int. Cl.5: **G06F 1/00**

(22) Date of filing: **31.05.90**

(43) Date of publication of application:
04.12.91 Bulletin 91/49

(84) Designated Contracting States:
DE FR GB

(71) Applicant: **International Business Machines Corporation**
Old Orchard Road
Armonk, N.Y. 10504(US)

(72) Inventor: **Holmes, Keith**
10 Llewellyn Close
Rathfarnham, Dublin 16(IE)

(74) Representative: **Bailey, Geoffrey Alan**
IBM United Kingdom Limited Intellectual Property Department Hursley Park
Winchester Hampshire SO21 2JN(GB)

(54) **Computer software protection.**

(57) A master copy 6 of a software file has within it a predetermined block of data 8. When a copy of the file is made that block of data within the copy file is located and overwritten with data identifying the copy file 12. When an unauthorised copy file is found the data identifying the copy file can be read and the source of the unauthorised copy may be traced. The invention is particularly suited to use with software distribution over a computer network in which details such as the time the copy file was made and the name of the authorised user can be embedded within the copy file.

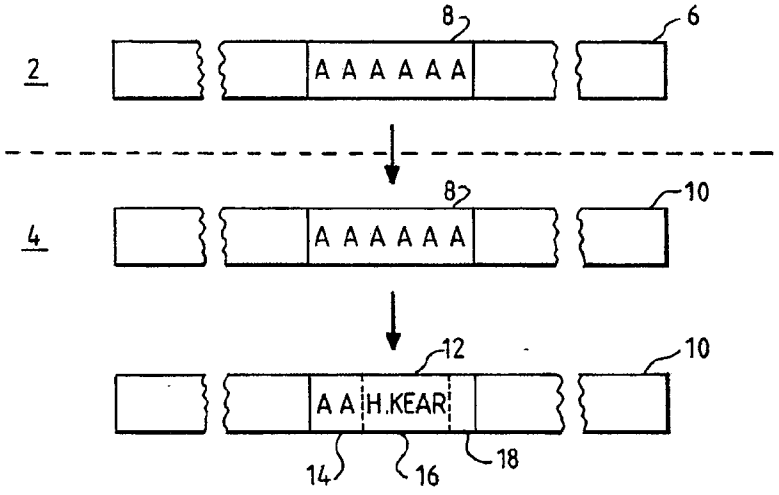

FIG. 1

EP 0 459 046 A1

This invention relates to the field of computer software protection. More particularly, this invention relates to combating the making of unauthorised copies of software.

Computer software whether in the form of computer programs or data files is a valuable asset. Much expense is involved in the production of such software and yet software is particularly vulnerable to theft. It is possible to make a copy of a piece of computer software in a matter of seconds using standard computer equipment and an appropriate medium such as a blank floppy disk. Having made a copy the original is completely intact and the unauthorised copy may be used by the thief without any payment to the software owner.

A large number of techniques have been proposed to combat the making of such unauthorised copies. Typically these techniques concentrate on the prevention of the production of a working copies of the software, e.g. by encryption, passwords or physical devices needed to enable use of the software. Examples of such techniques are described in British Published Patent Application No. 2154769, European Published Patent Application No. 302710, European Published Patent Application No. 67998 and International Published Patent Application No. WO 85/02310. Such techniques result in increased complexity and whilst offering a degree of protection are, in common with most forms of security, open to defeat by appropriate countermeasures. New security measures, particularly ones that can be simply and cheaply implemented, are desirable in trying to counteract unauthorised copying.

Viewed from one aspect the present invention provides a method of producing a copy file from a master file in a data processing system characterised by searching to locate a predetermined block of data within said copy file, and overwriting said predetermined block of data with data identifying said copy file.

The invention provides a technique whereby each copy of the software produced has data within it identifying that copy. If that copy is itself copied then the identifying information will be carried over into the unauthorised copy. If an unauthorised copy is discovered then the source of the unauthorised copy may be identified. The way in which this marking is carried out, by searching the master file or the master file for a block of data set aside for overwriting with the data identifying the copy file, is particularly easy to implement within standard computer hardware. There is no need for special purpose devices which bring with them increased complexity and expense. The data identifying the copy file may be written into the copy file with the same hardware that is copying over the rest of the master file. Furthermore, since the predetermined block of data may be positioned anywhere within the master and copy files it is difficult for an unauthorised copier to identify and remove the data identifying the copy file. Another advantage of the system is that a software file may be produced by a software vendor to include the predetermined block of data but use of that file will not require use of the technique of the invention. Accordingly, the same software file can be used in systems which do or do not implement the invention. The particular combination of elements comprising the invention provides a security technique which is surprisingly simple to implement and effective in use.

It will be seen that the invention is applicable wherever copies of software files are being produced, e.g. a single computer copying files onto floppy disks for distribution and sale. However, the invention is particularly applicable when said master file is stored on a first data processing system and said copy file is transmitted to a second data processing system. Such computer networks are becoming ever more common and bring with them a convenient way of distributing and maintaining software files. The invention is particularly suited for use in such networks since it is a relatively simple matter to add to the system the extra steps necessary to ensure that every copy of a software file distributed by the system may subsequently be uniquely identified. The data identifying the copy file could be added to the copy file either before or after transmission. Furthermore, producers of software files can include within them the necessary predetermined block of data which can be used to mark files distributed within the network and yet if desired the same version of the software file can be copied and distributed by conventional techniques without using the invention.

It will be appreciated that the data identifying the copy file could take many forms, e.g. it could be a serial number for that copy file with a central list held elsewhere giving further details of the copy file having each serial number. However, in preferred embodiments of the invention said data identifying said copy file includes one or more items of data identifying the time at which said copy file was made, the authorised user of said copy file, said first data processing system and/or said second data processing system.

Since the block of data to be overwritten may be positioned anywhere within the copy file a problem arises as to how to find the data identifying the copy file once it has been introduced. Accordingly, in preferred embodiments of the invention said data identifying said copy file includes a portion common to differing copy files so as to assist in detection of the location of said data identifying said copy file from within said copy file. A copy file may then be searched for the portion marking the

location of the data identifying the copy file when it is desired to recover that data.

A further feature of preferred embodiments of the invention which enhances their security is that the data identifying said copy file is encrypted. This renders less likely the possibility that a person browsing through the copy file would be able to recognise the data identifying the copy file. As a further safeguard against tampering the data identifying the copy file may include a checksum such that when the data identifying the copy file is recovered it can be checked against the checksum to indicated whether it has undergone unauthorised alteration.

Viewed from a second aspect the invention provides a method of identifying a particular copy file produced in accordance with the above characterised by searching said copy file to locate said data identifying said copy file and reading said data identifying said copy file. This is the complementary side to the first aspect of the invention in which data identifying the copy file was written into the copy file. This aspect relates to the reading of that data once it has been inserted.

Viewed from a third aspect the invention provides a master file having a predetermined block of data adapted to be overwritten with data identifying a copy file produced from said master file in accordance with the above.

Viewed from a fourth aspect the invention provides a data processing system for producing a copy file from a master file characterised by means for searching to locate a predetermined block of data within said master file, and means for overwriting said predetermined block of data with data identifying said copy file.

Viewed from a fifth aspect the invention provides a data processing system for identifying a particular copy file produced in accordance with the above characterised by means for searching said copy file to locate said data identifying said copy file, and means for reading said data identifying said copy file.

A embodiment of the invention will now be described, by way of example only, with reference to the accompanying drawings in which:

Figure 1 schematically illustrates the form of the master and copy files.

Figure 2 illustrates a network computer system which may embody the invention.

Figure 1 show a master file 6 stored within a first data processing system 2. The master file 6 has embedded somewhere within it a predetermined block of data 8. The block 8 does not play any part in the function of the software of the master file itself, rather its function is to provide a locatable space within the master file in which data identifying a copy file may be written. The block contains a predetermined sequence of code, in this example represented by 'AAAAAA'.

A copy of the master file is then transmitted to the second processor 4 which stored that copy file 10. The block 8 is copied with the rest of the master file 6 and so the copy file also contains a block 8 in the same position in the copy file 10 as the block 8 was within the master file 6.

The second processor 2 then searched through the copy file 10 to locate the block 8. It does this by looking for the occurrence of the sequence 'AAAAAA'. Once the block 8 has been located it is partially overwritten with the data identifying the copy file 12. This may comprise the name of the authorised user 16 for that copy file and a checksum 18. A portion 14 of the original sequence it left unaltered. This portion 14 will be common to a copy files and so enables the data identifying the copy file 12 to be located. Alternatively, a new sequence could be written into portion 14 for the purpose of enabling the data identifying the copy file to be located. Alternatively, a new sequence could be written into portion 14 for the purpose of enabling the data identifying the copy file 12 to be located.

The name could be the userid associated with the second processor or it could be the name of the user supplied to the second processor when it was initialised. The data identifying the copy file 12 may also comprise an identifier for the first processor, the second processor, and/or the time. Such data is commonly available within data processing networks. The checksum is performed on the data identifying the copy file 12 and the result added to the data 12. If the data identifying the copy file 12 is altered then the checksum will no longer be valid. This may be used to help identify attempts to tamper with the protection mechanism of the invention. The data 12 will also be encrypted in accordance with one on the well known algorithms such as those discussed in the book 'Security for Computer Networks' by D.W. Davies and W.L. Price, published by Wiley.

Having uniquely identified the copy file 10, this can then be released for use in the second processor 4. Any unauthorised copy made of the copy file 10 will carry with it the data identifying the copy file 10 from which it was made so that the source of the unauthorised copy may be subsequently traced.

The steps involved in this implementation of the invention are:

1. Transmit a copy of a master file from a first processor to a second processor.
2. The second processor searches through the received copy file to locate the predetermined block of data.
3. The second processor overwrites the pre-

determined block of data with data identifying that copy of the master file.

4. Release the copy file for use by the second processor.

Figure 2 illustrates a computer network of the type in which the invention may be implemented. The first processor 2 is a mainframe computer 20 with terminals 22 connected over a telecommunications link to a second processor 4 comprising a workstation 24 such as a personal computer. Software within the host processor 20 and workstation 24 controls the operation of the invention. The CPUs within the host and workstation under the control of appropriate software function as the means for carrying out the various functions required in operation of the invention.

The software to implement the invention can be written in any of the well known computer languages and, having described the function the software is to control, the writing of the software will be a matter of routine to those skilled in the art. It will also be appreciated that whilst the above has described a software embodiment of the invention it is theoretically possible to implement any software within hardwired logic and accordingly the marking of computer software files in the manner discussed could be carried out under the control of hardwired logic.

Claims

1. A method of producing a copy file (10) from a master file (6) in a data processing system (2, 4) characterised by searching to locate a predetermined block of data (8) within said copy file, and overwriting said predetermined block of data with data identifying said copy file (12).

2. A method as claimed in claim 1, wherein said master file is stored on a first data processing system (2) and said copy file is transmitted to a second data processing system (4).

3. A method as claimed in claim 2, wherein said data identifying said copy file includes one or more of data identifying said first data processing system and data identifying said second data processing system.

4. A method as claimed in any of claims 1, 2, or 3, wherein said data identifying said copy file includes one or more of data identifying the time at which said copy file was made and the authorised user of said copy file.

5. A method as claimed in any preceding claim, wherein said data identifying said copy file includes a portion (14) common to differing copy files.

6. A method as claimed in any preceding claim, wherein said data identifying said copy file includes a checksum (18) of said data identifying said copy file.

7. A method as claimed in any preceding claim, wherein said data identifying said copy file is encrypted.

8. A method of identifying a copy file produced in accordance with the method as claimed in any preceding claim characterised by searching said copy file to locate said data identifying said copy file and reading said data identifying said copy file.

9. A master file having a predetermined block of data adapted to be overwritten in accordance with the method as claimed in any of claims 1 to 7.

10. A data processing system for producing a copy file from a master file characterised by means for searching to locate a predetermined block of data within said master file, and means for overwriting said predetermined block of data with data identifying said copy file.

11. A data processing system for identifying a copy file produced in accordance with the method as claimed in any of claims 1 to 7 characterised by means for searching said copy file to locate said data identifying said copy file, and means for reading said data identifying said copy file.

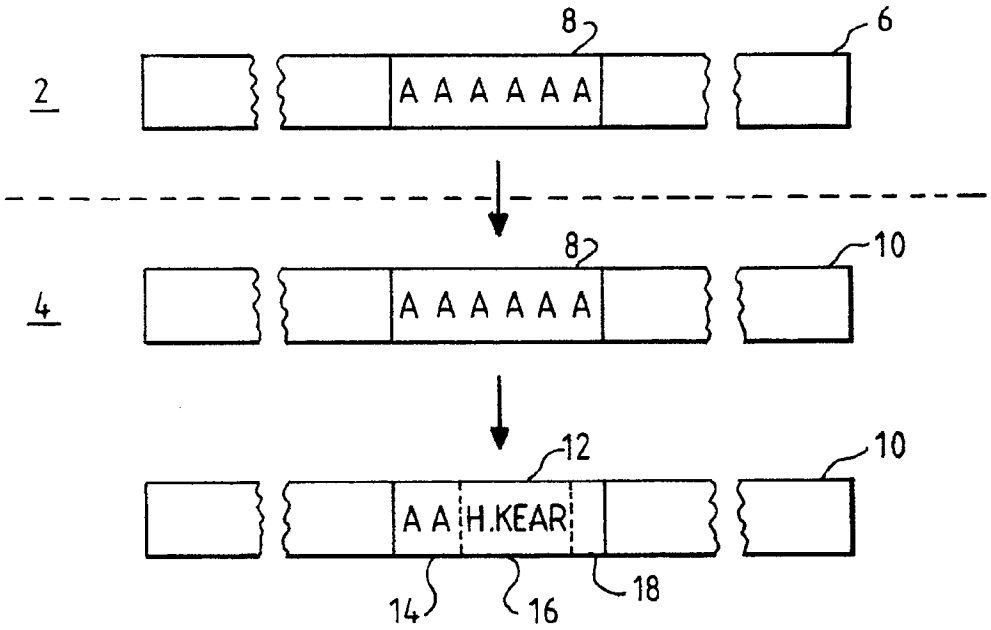

FIG. 1

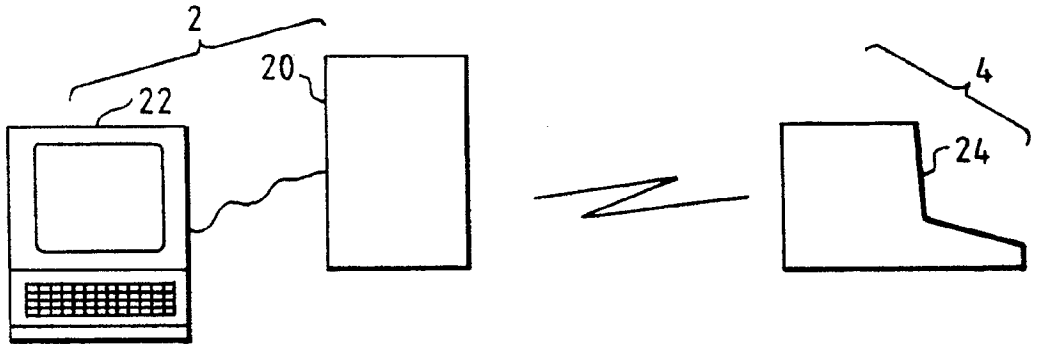

FIG. 2

European Patent Office

EUROPEAN SEARCH REPORT

Application Number

EP 90 30 5964

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.5)
A	FR-A-2 541 014 (CII HONEYWELL BULL) * Page 5, line 20 - page 7, line 27 *	1,10	G 06 F 1/00
A	IBM TECHNICAL DISCLOSURE BULLETIN, vol. 28, no. 2, July 1985, page 704, New York, US; "Computer program identification" * Complete document *	1,4,8,10, 11	
D,A	WO-A-8 201 273 (LÖFBERG) * Page 4, line 30 - page 5, line 13; page 6, lines 12-20 *	1,10	
A	US-A-4 748 561 (BROWN) * Column 1, line 58 - column 3, line 24 *	1,10	

TECHNICAL FIELDS SEARCHED (Int. Cl.5)

G 06 F 1/00

The present search report has been drawn up for all claims

Place of search	Date of completion of search	Examiner
The Hague	11 February 91	MOENS R.A.A.

CATEGORY OF CITED DOCUMENTS

X: particularly relevant if taken alone
Y: particularly relevant if combined with another document of the same catagory
A: technological background
O: non-written disclosure
P: intermediate document
T: theory or principle underlying the invention

E: earlier patent document, but published on, or after the filing date
D: document cited in the application
L: document cited for other reasons

&: member of the same patent family, corresponding document